Investigating Approaches for Secure Data Aggregation in Wireless Sensor Networks

Vivaksha J. Jariwala
Assistant Professor
Computer Engineering Department
CKPCET, Surat
+912612728282
vivakshajariwala@gmail.com

Devesh C. Jinwala
Professor
Computer Engineering Department
SVNIT, Surat
+912612201593
dcjinwala@gmail.com

ABSTRACT
The Wireless Sensor Networks (WSNs) protocols commonly use in-network processing to optimize the communication costs. In-network processing involves processing of the sensed data on-the-fly during the course of the communication to the base station. However, due to the fusion of data items sourced at different nodes into a single one, the security of the aggregated data as well as that of the aggregating node, demands critical investigation. One of the approaches to ensure secure data aggregation is to use encrypted sensor data for processing, using homomorphic encryption. As per our observation, an integrated solution that offers all the necessary security attributes viz. confidentiality, privacy, integrity and robustness is not found in the literature. Hence, our research here is aimed to propose an approach that uses homomorphic encryption and appropriate data integrity mechanisms to offer confidentiality, privacy, data integrity and robustness for secure data aggregation in wireless sensor networks.

Categories and Subject Descriptors
K.6.5 [**Management of Computing and Information System**]: Security and Protection

General Terms
Security.

Keywords
Privacy homomorphism, in-network processing, secure data aggregation, elliptic curve cryptography.

1. INTRODUCTION
As part of our literature survey, we observe that there are several homomorphic encryption algorithms [1],[2],[3],[4],[5],[6] already proposed for conventional networks and a few even ported to the wireless sensor network environment, but that provide only confidentiality. In this research, our focus is to propose an approach that uses homomorphic encryption and appropriate data integrity mechanisms to offer confidentiality, privacy, data integrity and robustness for secure data aggregation in wireless sensor networks.

Our first step in this direction was to augment TinySec by methodologically investigating a better candidate for homomorphic encryption. Initially, we analyze the existing homomorphic encryption algorithms (available either for conventional or wireless sensor networks) and benchmark them [7]. Subsequently we also adapt, port, and benchmark the ECC based algorithms for homomorphic encryption in WSNs [8]. Our results proclaim EC-OU [9], as a better alternative for secure data aggregation, in the TinyECC, as compared to the existing EC-IES. In the process, we also augment the TinyECC library by providing support for the various ECC based homomorphic encryption algorithms.

Proceeding there from, we realized that any security solution that does not integrate a data aggregation topology is of no use, actually. Hence, we explored the prevalent data aggregation topologies and realizing the tree topology is the most widely used, we integrated EC-OU into tree topology for secure data aggregation using privacy homomorphism. Our approach achieves confidentiality and privacy for secure data aggregation in WSNs. To the best of our knowledge, ours is the first experimental evaluation of integrating ECC based privacy homomorphic encryption algorithm EC-OU into tree topology to achieve confidentiality and privacy for secure data aggregation for WSNs.

However, any encryption algorithm for Secure Data Aggregation, without the support for data integrity is meaningless. Hence, our further research work focuses on investigation of the techniques for supporting data integrity; that we intend to integrate with our earlier benchmarked algorithm for confidentiality. The approaches to provide data integrity can be either cryptography-based or non-cryptography-based. Our focus here is only on cryptographic approaches.

EC-DSA is an example of a standard signature based algorithm for data integrity that is our primary focus in this research. Towards fulfilling the aim of proposing an integrated secure solution for data aggregation, we implement, analyze, integrate and evaluate the EC-DSA with our earlier benchmarked algorithm viz. EC-OU. In addition, we also observe two more variants of EC-DSA already published in the literature viz. one that focuses on limited resource on sender side and the other that focuses on limited resource on receiver side. We have also empirically evaluated these two variants in TinyECC [2], thus making our proposed solution more versatile.

Further, we also observe that the security of EC-DSA [10] and its proposed two variants is based on EC-DLP and random number it uses to generate the signature. Thus, one of the obvious limitation of the basic EC-DSA is that if an EC-DSA cryptosystem encounters the same random number (as was used

in a previous run of the EC-DSA), to generate two different signatures, the adversary can know the private key and generate false signatures. One of the obvious and simplest solutions to deal with the problem is to use multiple random numbers. We implement two different variants of EC-DSA viz. one using two random numbers and the other using three random numbers to improve the security strength of the same and empirically evaluate the resource overhead due to the same using RAM, ROM and energy as the metrics. However, when using additional random numbers to enhance the security strength, a vital issue that crops up is viz. how many such invocations of random numbers to use? To answer the same and improve intrinsic strength of EC-DSA, we also propose a solution that uses the set membership data structure viz. bloom filter [11]; to avoid repetition of a random number used in EC-DSA. The only argument against the usage of the proposed variant could be if at all we have a strong random number generator that ensures non-repetition, is it necessary to employ this variant. However, in that case, EC-DSA remains dependent on the implementation to be secure – the algorithm lacks intrinsic security strength. Hence, our proposal is justified in that it enhances the intrinsic security strength of the EC-DSA algorithm without assuming any guarantees from the underlying implementation. Our results clearly show that our variant of EC-DSA is suitable for any application demanding integrity support in resource constrained environment of WSNs. We have also incorporated novel variant based on bloom filter [11] with our proposed approach of secure data aggregation.

In addition to that, to counter the overhead due to the digital signatures, we also propose a MAC based hop-by-hop authentication scheme for secure data aggregation with our earlier framework. To support the authentication, we also analyze various kind of MAC i.e. Conventional MAC, Aggregate MAC [12] and Homomorphic MAC [13]. Moreover, we also propose our own variant of Homomorphic MAC to improve the security strength for secure data aggregation in WSNs. Thus, with the support for EC-OU based confidentiality, improved and optimized EC-DSA based digital signature for data integrity and Homomorphic MAC based alternative to support the same attribute, we intend to make our proposed framework more versatile.

However, topology construction and key management is also equally important part of Secure Data Aggregation. Therefore, to fulfill that, we also proposed zero configuration protocol for secure data aggregation that provides topology construction and key management in addition of privacy, confidentiality, integrity and robustness.

Hence, our proposed approach for secure data aggregation provides the following features. A) confidentiality and privacy B) confidentiality, privacy and EC-DSA based end-to-end integrity C) confidentiality, privacy and novel bloom filter based end-to-end integrity and D) confidentiality, privacy and MAC based hop-by-hop integrity. E) various ways of integrity including MAC, aggregate MAC, homormophic MAC and improved homomorphic MAC and F) zero configuration protocol that provides topology construction and key management in addition of privacy, confidentiality, integrity and robustness.

2. REFERENCES

[1] S. Peter, D. Westhoff, and C. Castelluccia. A survey on the encryption of convergecast-traffic with in-network processing. *IEEE Transactions on Dependable and Secure Computing*, Vol. 7, No. 1, 2010.

[2] A. Liu, P. Kampanakis, P. Ning. TinyECC: Elliptic curve cryptography for sensor networks. In Proceedings of the *International Conference on Information Processing in Sensor Networks*, pp. 245-256, 2008.

[3] Osman Ugus, Alban Hessler, Dirk Westhoff. Performance of Additive Homomorphic EC-ElGamal Encryption for TinyPEDS. In: *GI/ITG KuVS Fachgespräch*, Drahtlose Sensornetze, RWTH Aachen, 2007.

[4] Xiaoyan Wang; Jie Li; Xiaoning Peng; Beiji Zou. Secure and Efficient Data Aggregation for Wireless Sensor Networks. In Proceeding of the *Vehicular Technology Conference Fall (VTC 2010-Fall)*, 2010 IEEE 72nd , pp.1-5, 6-9 Sept. 2010.

[5] Poornima, A.S.; Amberker, B.B. SEEDA: Secure end-to-end data aggregation in Wireless Sensor Networks. In Proceeding of the *7th International Conference of Wireless And Optical Communications Networks (WOCN)*, pp.1-5, 6-8 Sept. 2010.

[6] Jacques M. Bahi, Christophe Guyeux, and Abdallah Makhoul. Efficient and Robust Secure Aggregation of Encrypted Data in Sensor Networks. In Proceedings of the *2010 Fourth International Conference on Sensor Technologies and Applications (SENSORCOMM '10)*, IEEE Computer Society, Washington, DC, USA, pp. 472-477, 2010.

[7] Vivaksha Jariwala, Devesh Jinwala. Evaluating Homomorphic Encryption Algorithms for Privacy in Wireless Sensor Networks. *International Journal of Advancements in Computing Technology*, Vol. 3, No. 6, pp. 215-223, 2011.

[8] Vivaksha Jariwala, Asha Munjpara, Devesh Jinwala, Dhiren Patel. Comparative Evaluation of ECC Based Homomorphic Encryption Algorithms in TOSSIM for Wireless Sensor Networks. In Proceedings of the *National Workshop on Cryptology*, Cryptology Research Society of India and VIT, Vellore, TN, pp. 1-14, 2012.

[9] P. Paillier. Trapdooring Discrete Logarithms on Elliptic Curves over Rings. In Proceeding of the *Ann. Int'l Conf. Theory and Application of Cryptology and Information Security (ASIACRYPT '00)*, pp. 573-584, 2000.

[10] Don Johnson, Alfred Menezes and Scott Vanstone. The Elliptic Curve Digital Signature Algorithm (ECDSA). *International Journal of Information Security*, Vol. 1, No. 1, Springer-Verlag, pp. 36-63, 2001.

[11] Bloom, B. Space/time Trade-offs in Hash Coding with Allowable Errors. *Communications of the ACM*, Vol. 13, No. 7, pp.422-426, 1970.

[12] Katz, J., Lindell A. Aggregate Message Authentication Codes. *Malkin, T.G. (ed.) CT-RSA 2008. LNCS*, Springer, Heidelberg, Vol. 4964, pp. 155–169, 2008.

[13] Agrawal, S., Boneh D. Homomorphic MACs: MAC-Based Integrity for Network Coding. In Proceeding of *ACNS 2009*, LNCS, Vol. 5536, pp. 292–305, 2009.